ON THE FUTURE OF BITCOIN AND ALTCOINS AS CURRENCIES, TOKENS FOR SMART CONTRACTS, AND INSTRUMENTS OF COMMITMENT (IOCS): SOME CONSIDERATIONS REGARDING BLOCKCHAIN APPLICATIONS

Wolfgang Eibner
Kurt Rätzsch, Antonio Schulz, André Rolapp
University of Applied Sciences Jena[1]

Abstract

In the article we discuss following hypotheses:
Thesis 1: „Private Cryptocurrencies will not be seen as an alternative to Fiat-Money in the near future or any time soon."
Thesis 2: „Initial Coin Offerigs (ICOs) can increasingly become an alternative to traditional Venture Capital Financing and Token might enable to build smart contracts on a decentralized infrastructure."
In the article we explain Blockchain technology and its possible applications in a very wide range. Also are shown main cryptocurrencies in their functions as possible future currencies, as platform token, and utility token necessary for Smart Contracts, or equity token, especially for Initial Coin Offerings. A main part of the article is the discussion of possible risks in the these applications of cryptocurrencies or token, referring explicitly to technical risks, economical risks like the stability of the financial markets (volatility, deflation), but also the severe problem of manipulated markets, supplemented by some considerations on legal issues.

Keywords: Blockchain, Bitcoin, Altcoin, Initial Coin Offerings, Possibility to replace Fiat-Money by Cryptocurrencies, Token for Smart Contracts, Future role of ICOs as an Alternative to IPOs for Equity Capital Acquisition.

JEL Classification: E42, E51 (referring also to A10, E31, O16, Z00)

1 Cryptocurrencies

1.1 Vision and Working Hypotheses

The vision of a digital currency performing anonymous money transactions is not new: as far back as 1999, Milton Friedman envisioned the transfer of funds from A to B on the Internet without the transaction partners knowing one another or without a record of where the money came from. [45, Video of the Interview, cited in minutes following minute 14:40)]

[1] Prof. Dr. rer. pol. Wolfgang Eibner, Department of Industrial Engineering, Ernst-Abbe-University of Applied Sciences, Jena, Carl-Zeiss-Promenade 2, 07745 Jena, Germany, Wolfgang.Eibner@eah-jena.de.
This contribution was written with the gratitude of candes. M.Sc. Wirt.-Ing. Kurt Rätzsch, Antonio Schulz, André Rolapp.

In 2008, the white paper “Bitcoin: A Peer-to-Peer Electronic Cash System” [65, p. 1] was published under the pseudonym Satoshi Nakamoto, whose identity is still not known to this day. It is considered a response to the financial crisis of 2007 and the foundation document of the virtual currency of the Bitcoin. Nakamoto described a payment system without intermediaries serving as a trustworthy institution. He described a system which is based on cryptographic proof rather than trust and allows two parties to deal directly with one another.

Bitcoin was the first cryptocurrency; other, alternative cryptocurrencies are lumped together under the umbrella term “alternative coins,” or “altcoins.” A Bitcoin or other altcoin networks thus set in motion the transfer of value without intermediaries, which otherwise is only possible with cash and among parties who are physically close to one another. Thanks to cryptographic proof and the consensus of the network participants, financial institutions are no longer required. This “elimination” of financial intermediaries—specifically of commercial banks involved in handling payment transactions—is the central new feature of Bitcoin and the new technology on which it is based, the so-called blockchain.

The participants in the Bitcoin network are in a distributed network: all of the participants have equal rights and hence the same datasets (consensus). Such a distributed network is utterly decentralized—contrary to a centralized network which, e.g., has only one database, or a decentralized network that is realized via different data processing centers, as for instance a cloud.

In contradistinction to conventional so-called fiat currencies, such cryptographically encoded cryptocurrencies are not regulated and controlled by central institutions (e.g., the central banking authority) but are typically issued only by natural and legal persons and managed within a specific framework. [2]

Payment transactions using these kinds of cryptocurrencies thus take place directly between the individual users of the pertinent cryptocurrency, i.e., without entities such as banks or service providers like PayPal serving as intermediaries. In theory this allows for extremely inexpensive and fast transactions. Plus, the money supply cannot be randomly increased, as is the case with fiat currencies.

However, conventional currencies and cryptocurrencies share a very important feature: their value is defined through their so-called usage value or the trust put into the respective means (of exchange). The technology used with cryptocurrencies which engenders this trust is the blockchain, which is therefore examined more closely below.

As the boom of the so-called crypto market showed, specifically in the period between September and December 2017, the innovation of the blockchain and the currencies it generates is for many, especially younger people, a great vision of decentralized decisions and bank-independent value transactions.

---

[2] The concept of fiat currencies, derived from the Latin word "fiat" (= it will be created), refers to all modern, unfunded currencies subject to (unlimited) money creation by central Bank (primary money) or commercial banks (secondary money). Especially the representatives of the Austrian School of the national economy, as in particular Ludwig von Mises, Friedrich August von Hayek and Murray N. Rothbard or the US economist Irving Fischer fear that the modern money uncontrolled propagation via the central bank or commercial banks will lead to an eventual loss of wealth and the resulting expropriation/impoverishment of the population. This is a central argument of many followers of the decentralized and not arbitrarily propagatingable Cryptocurrencies, that they want to replace the recent (fiat) money by cryptocurrencies.

The following analysis is based on two central working hypotheses which will be examined below:

Thesis 1: **"Private cryptocurrencies are inconceivable as an alternative means of payment in the foreseeable future."**

Thesis 2: **"Increasingly, ICOs can become an alternative to conventional venture capital financing and tokens the driving force to build smart contracts on a decentralized infrastructure."**

1.2 Blockchain

1.2.1 Transaction Process

The blockchain is a novel technology for the verification of data transactions [85, p. 6]. The name is directly derived from the specific characteristics of this technology: data blocks containing transaction information are strung together in linear, chronological sequence. [73, pp. 58]

The technology of the blockchain is considered to be safe and, above all, error-resistant. It possesses the potential to resolve the problem of trust between the different value creation partners with respect to transactions of monetary value, the exchange of data and the processing of contracts.

To transfer bitcoin or altcoin units among different so-called e-wallets (in analogy to conventional financial transactions also regarded as *accounts*) first a transaction notice must be generated and announced in the network. Numerous user-friendly Web applications are already available for this. They greatly simplify the process and are actively or passively connected to the network. [73, pp. 169]

Similar to a broadcast, this transaction notice reaches the active participants in the Bitcoin network whose job it is to check incoming transaction notices using cryptographic algorithms and collecting them in a data block.

Another function of the active network participants is to solve an arithmetic problem once the transactions have been collected in a data block. It is no classic arithmetic problem, however, but rather a trial-and-error procedure that requires arithmetic. Once the problem has been solved, the newly created block of the respective active participant—also called a "miner"—is posted in the network, again checked for validity by the other participants, and finally added to the most current version of the blockchain.

After about another ten minutes (the average block generation time in the Bitcoin network) the first confirmation is issued from the Bitcoin network that the respective amount has been credited. [4]

1.2.2 Safety Mechanisms

The structure of the blockchain makes the technology far safer than conventional encryption technologies. To ensure this, various safety mechanisms are used in the protocol.

Since the individual data blocks are *referenced* among one another, previous network transactions cannot be manipulated without this being noticed.

The property of unobstructed and full *transparency* of all transaction details of public blockchains—including, e.g., credit and "account balances" as well as the amount of

money or bitcoins in circulation—creates trust in the network and ensures that one's own transactions can always be traced and monitored. At the same time, however, these sensitive data cannot be connected to specific individuals but only to pseudonyms of the network participants, which makes it very difficult to assign them to real persons.
Thanks to the *decentralized* character of the network, the transactions can be checked—in the case of the bitcoin network by thousands of network nodes around the globe. As a result, no trust in an intermediary party is required. [73]

1.3 Smart Contracts and Distributed Apps

In 2014 Vitalik Buterin expanded Nakamoto's vision and created a blockchain-based platform in Ethereum which allows for the decentralized processing of "smart contracts," which in turn constitute the foundation for so-called distributed applications.
At the most elementary level, smart contracts are programs which, like written contracts, contain specific contractual terms for all parties involved and can trigger an automated performance of the contract when a service is delivered (for instance by the customer or client). Schematically speaking, smart contracts are based on IFTT (if this then that) logic. This makes for all kinds of scenarios. [18]
At the same time an extremely significant blockchain-based application has developed by now in the **tokens**. Tokens can be programmed via smart contracts on "dApp-capable" blockchain platforms such as Ethereum. They constitute a fundamentally new cryptocurrency, as it were, which uses the infrastructure—and hence also the blockchain—of a foreign platform. [3] Coins such as bitcoin, ether or NEO, on the other hand, use their own infrastructure and represent the native cryptocurrency of their own blockchain.
This has numerous advantages: the programming and generation process of a new cryptocurrency is considerably reduced. Private individuals and companies that want to use their own cryptocurrency no longer need to build their own infrastructure and provide resources. Rather, tokens can now be produced within a few minutes via a large number of Web applications and in a way that even laypeople can understand. (An example therefore can be found on the webside https://tokenfactory.com.)
With the newly created tokens all network transactions are performed via the underlying platform (e.g., the Ethereum blockchain) and transaction fees are also paid in the native cryptocurrency (e.g., Ether). Consequently, the transactions, account balances, and written smart contracts are also accessible on this blockchain. In this way the value of the native currency is collateralized to a certain degree by the underlying platform. [17]
Even as a token is being programmed, numerous general conditions can be irreversibly established, such as the limitation of the total number of tokens that will be in circulation in the future.

1.4 Overview of Types and Market Capitalization of Cryptocurrencies

1.4.1 Types of Cryptocurrencies

Classifying cryptocurrencies as shown, e.g., in figure 1 is difficult as no established and generally recognized definitions of terms exist as yet and a token can easily satisfy various requirements. Every day new cryptocurrencies are being generated: CoinMarketCap lists 1,890 different cryptocurrencies as of 8/26/2018. [25]

Therefore, figure 1 constitutes one of several ways to classify cryptocurrencies. Under the term "token" it also groups together cryptocurrencies which are only used as *means of payment*. For instance, Bitcoin (BTC), IOTA, and Monero (XMR) were only grouped together under *Cryptocurrencies*, even though the purpose of the payment function is or may be the remuneration for specific services (such as most notably in the case of IOTA, which has a payment function for smart contracts in the Internet of Things—cf. also chapter 3.3).

As the name implies, *platform tokens* make their blockchain available as a platform for diverse applications: other systems build on the platform (for instance ICOs or dApps—decentralized applications) in order to create a new cryptocurrency on the basis of this existing infrastructure, such as, specifically, Ethereum (ETH) or tokens as means of payment, and to perform smart contracts. Even though platform tokens can be used as means of payment, this is not necessarily their intended purpose.

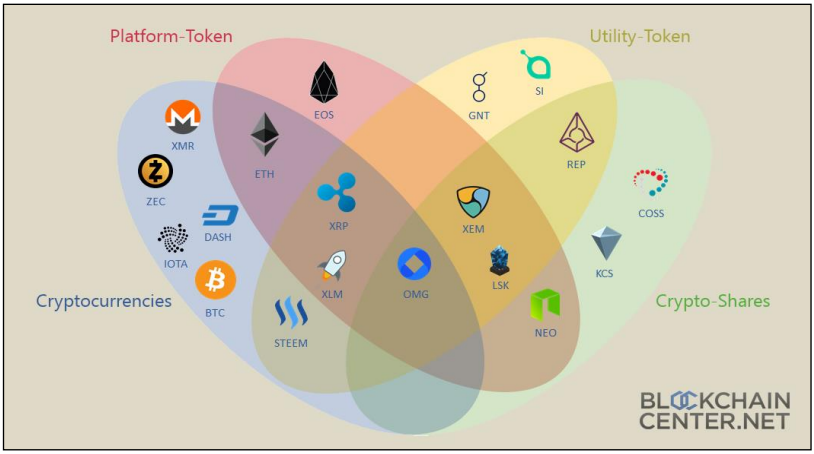


Figure 1: Overview of relevant cryptocurrencies [16]

By contrast, the purpose of *utility tokens*, such as specifically Augur, Steem, Bancor, Golem, or Sia, is to offer applications which are programmed on a dApp platform. (To dApp see: [79, pp. 83].) They have a clearly defined function of any application environment at the outset, for example as payback points or the payment of resources provided but not used. Like platform tokens, utility tokens have no intended use outside of the system in which they exist (except for speculative transactions).

Crypto shares, also called *security or equity tokens*, such as specifically NEO, Binance coin, Kucoin shares, or Coss represent to a certain degree shares in a company, network, or single project. This type of token, however, has no inherent value and typically only serves speculation purposes. Generally owners receive a regular kind of dividend or, in the case of NEO, the asset value bears interest. Yet it must be emphasized that no legal foundation—as, for instance, for securities—exists for this as yet. [16]

Appendix I presents a selection of those cryptocurrencies that show the highest market capitalization (as of mid-2018) and therefore currently have the greatest relevance and

largest daily user base. Remarkably, with the exception of the token OmiseGo, all cryptocurrencies listed have their own network, and their primary goal tends to be to serve as a means of payment.

1.4.2 Market Capitalization

Figure 2 compares the market cap of cryptocurrencies and gold, shares, and bonds for 2016.

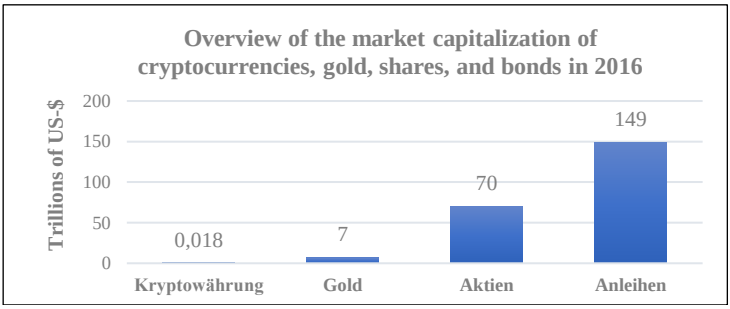


Figure 2: Overview of the market capitalization of cryptocurrencies, gold, shares, and bonds in 2016 [24, 42, 81, 84]

Despite the attention they have received, the market cap of the cryptocurrencies is very low compared to gold, shares, and bonds. It is still in the development and acceptance phase.
Figure 3 shows the development of the market cap of cryptocurrencies between 2015 and August 2018.

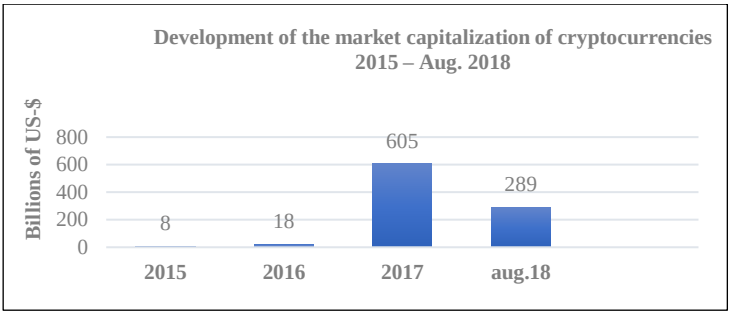


Figure 3: Development of the market capitalization of cryptocurrencies 2015–Aug. 2018 [24]

Starting with a total trading volume totaling just US-$8 billion in 2015, the cryptocurrencies reached their maximum market cap to date in December 2017 with the peak of the crypto boom so far at US-$605 billion. Since December 2017, the drop in demand for this form of investment has led to a steady decline of the market cap; in August 2018 it was less than US-$300 billion.

Appendix II shows the three exemplary trading platforms for cryptocurrencies: Bitcoin.de from Germany, Coinbase.com from the USA, and Bitfinex.com from China and Hong Kong, which is currently the world's second-largest trading platform.

2 Initial Coin Offerings (ICOs)

2.1 Definition

In addition to the payment function of cryptocurrencies, the use of blockchain technology is gaining in importance for aspects other than "only" as means of payment: the so-called ICOs.

The term "initial coin offering" is derived from "initial public offering" and also denotes the initial issue of asset values by a company. However, here it is not company shares, as is the case with the latter, but only the initial issue to investors of the cryptocurrency created by the respective company. This implies that, contrary to the purchase of securities, an investor's tokens generally do not signify ownership in the company: ICOs neither entitle their bearers to dividends nor do they give them voting rights. [50]

Initially almost the sole purpose of ICOs was to introduce new cryptocurrencies, announce them to the public, and raise funds. By now, however, the range of applications of ICOs has expanded: funding via ICOs is also of increasing interest to existing companies on a project basis and can therefore generally also be viewed as a method for initial funding of startups/companies and individual projects via crowdfunding or the issue of tokens as tradable and potential asset values.

2.2 Process of an Initial Coin Offering

Typically an initial coin offering starts with the announcement of a project to be financed in this way and the requisite marketing activities to approach as many prospective investors as possible. The initiating company or project team furthermore decides on a dApp platform, such as Ethereum, on which the ICO is to take place. For realization see for example [79], pp. 63].) Once this decision has been made, the required smart contracts are implemented on the blockchain via the proper software, and a contract address is generated. This contract address is a common hash address for the account, but also for triggering automated activities in communications with it which were previously defined in the source code. [41]

In this case the contract address is important in that it determines the pro rata distribution of the new cryptocurrency to the investors. To this end the supporters/investors send an amount of the native currency (e.g., Ether) which they are usually free to choose, to the contract address and in exchange are credited the number of tokens corresponding to that amount on their (Ether) address.[3]

With a market cap of a few hundred billion euros, the ICO and cryptocurrency market still seems to be relatively insignificant, but it is developing at remarkable speed: in September 2017 alone, 37 ICOs collected over US-$850 million, which resulted in a total of US-$1.32 billion for the quarter. [88, p. 17] In 2018 the amount was US-$6.5 billion from January to April [69, p. 12, figure 1], but with the drastic fall in prices in the crypto market the number of issues per month is in sharp decline again. [82, p. 2]

[3] An address for example has the form: 2JIvAFJqQ3i2JNMoZjkCV0071xBUZjXYxQ

2.3 Opportunities

Especially in a direct comparison with the tried and tested IPOs, the initial coin offering entails numerous advantages which are concisely listed below:

1. *The capital procurement process is greatly simplified:* The bureaucratic hurdles and the effort involved in changing the legal form of a company are relatively high when it becomes listed on the stock exchange. Here an ICO can offer an enormous cost advantage.
2. *Comprehensive know-how is no longer required:* Nowadays it only takes basic IT knowledge to implement a project-based ICO with intuitive tools and Web applications.
3. *The blockchain and hence also the smart contracts stored on it have an unalterable, transparent character*: An offer of tokens (the supply) which is defined at the outset can no longer be altered and can be viewed, along with the entire source code of the ICO, at any time on the public blockchain of the respective platform.
4. *Expanded access to investment opportunities:* The automated issue of tokens via public blockchains drastically increases the number of potential investors. Global access is generated, of which both the investors themselves and the company / project team benefit. [50]

2.4 Central Problems

Information asymmetry

Currently it is often a so-called white paper published by the entrepreneurs / project team that serves as the basis of an ICO investment decision of private individuals. A white paper is a position paper in which the team provides information on the project vision, the product, the planned development process, the targeted market, and/or the people involved. Here the decentralized and up until now still largely unregulated character of this market becomes a crucial disadvantage: there are no standards, guidelines, or norms for such a position paper. Plus, these ICOs are only now beginning to be monitored by government authorities, such as the SEC or BaFin (German Financial Authority).

A study by the University of Luxembourg has revealed that only about 25% of the white papers examined shed light on the financial situation of the company/project. Potential supporters are often given such few details that it is impossible to make an informed investment decision. [88, p. 15]

Furthermore, less than one-third of white papers offered notes on the applicable law, and 55% of the position papers contained no information whatsoever on the identities or addresses of the initiators.

Without these basic data, it is nearly impossible to assert legal claims. After all, if you cannot even identify, let alone locate, your contractual partner, a claimant's hands are tied even if he or she lives in a country with an intact legal system. [88, p. 16]

In the future, ICOs will therefore have to become part of a legal and control framework that is adequate to the risk posed by these types of business.

Improper use of assets
Obviously, despite all the advantages of the protection of privacy blockchains offer, their inherent decentralized character and the anonymity of the network participants can also relatively easily lead to an improper use of the assets collected by way of an ICO. What is more, due to the largely unregulated character of ICOs and cryptocurrencies, the seeming protection offered by the anonymized system adds to dishonest initiators' sense of being safe. In the past this has already resulted in numerous so-called exit scams (the untraceable digital "disappearance" of crypto or ICO accounts) as well as snowball systems. [88, p. 15]

3 Areas of Application of ICOs and Tokens

3.1 Overview

The currently most practical types of application of the blockchain can be found in the finance industry. An overview of the specific blockchain solutions shows that the different projects can be mostly allocated to the following areas of application [70, p. 16]:

1. Cryptocurrencies: The blockchain application serves as a transaction protocol for different cryptocurrencies, such as Bitcoin, Ethereum, or Monero.
2. Business networks: The blockchain is applied in the field of smart contracting and data exchange. Ethereum specifically can be found here as a smart contract application.
3. Smart contract communication by nonhuman agents in the Internet of Things: Here IOTA is an example of an expedient technology.
4. Banking: The blockchain is used in financial transactions. The most notable of these applications are Ripple, the leader in this area, and the relatively new Corda.[4]

Below, the specific wide application range of the blockchain technology is presented by way of examples: it can be employed in all areas dealing with the collection, documentation, or performance of transactions of any kind of contracts or objects. [74]

3.2 Finance Industry

Currently the finance industry is the sector that shows the busiest blockchain-related activities. Even though invoices are provided and transactions are conducted digitally via online banking and other e-payment systems, performing standard financial transactions is still quite time- and resource-consuming. Banks are needed for this as intermediaries and hence prevent the transactions from being anonymous.
Blockchains have the potential to reduce the disadvantages concerning time and cost of the currently centralized systems and to eliminate the necessity of an intermediary. This is achieved through shorter processing times and can also diminish the foreign exchange risk involved in international transactions. The blockchain-based payment systems

[4] The core of Corda is a network of local smart contracts, which only act between two or more direct communication partners. In comparison to Blockchain, Corda does not distribute the entire list of all, but only the confirmed transactions on the nodes: See [62])

increase safety and the user's privacy. This is possible because the transaction is initiated without the need to provide any bank details.
Another highly promising area of application is securities transactions. By shortening processing times, cost and complexity of the transactions can be reduced to minutes or seconds, since the parties deal directly with one another. This diminishes the operational and contracting risks, and the minimum equity requirement of banks can be reduced as well, which would in fact help stabilize the finance system. The credit and liquidity risk could be effectively eliminated, as due the way the blockchain system works, having the necessary liquid funds would be ensured prior to the trading process. Furthermore, using smart contracts would allow for performing transactions without invoices. The blockchain protects the contract content (so-called service level agreements [SLAs]) and the smart contracts monitor the performance of the contract via so-called if–then conditions. As a result, automated transactions are possible. [70, p. 17]

3.3 Internet of Things (IoT)

A central element of the IoT is the digital interlinking of physical objects by way of smart services. The objective is to improve man–machine or machine–machine interactions.
Central coordination of the IoT, however, is nearly impossible, especially since the aim is for the objects to become autonomous. This autonomy and decentralized coordination can be achieved with the blockchain technology. Smart contracts open up the possibility for machines to make agreements autonomously, adherence to which is ensured in both directions (among machines as well as between people and machines). The cryptocurrency IOTA is to allow for precisely this communication among machines without any human involvement. [57]
The idea of a refrigerator autonomously ordering and paying for its content has long since ceased to be merely a vision, and this is precisely what IOTA accomplishes. Services can be billed directly to the user, and the money received can be stored decentrally in a "wallet." Thus future business models are conceivable where autonomous machines offer people their services, earn money directly, announce their need for maintenance autonomously, and perform billing and payments in both directions. Taxing the work of machines—an issue discussed in politics—would be easy to do, as part of the machine's income can be paid to the government. [70, p. 18]

3.4 Smart Contracts Using the Example of Supply Chain Management

An interesting field of application for the implementation of the blockchain technology is supply chain management. Due to the large number of value creation partners (suppliers, manufacturers, retailers, logistics and financial service providers) a system is required that ensures safe data exchange.
Nowadays the physical performance of logistical process services of the supply chain is already approaching the limits of what is possible. Even so, the financial transactions are too slow, particularly due to paper invoices and their decoupling from the service performance process. The blockchain offers the potential to simply integrate them into the existing process and conduct the billing process with the networked partners via smart contracts.
Figure 4 shows a blockchain-based supply chain network with several partners in simplified form.

The blockchain works as a distributed database and stores publicly as well as irreversibly all relevant information the smart contracts require. As the executing computer program, the smart contracts check adherence to the content of the contract and, when all agreements have been kept, the financial transactions autonomously (without human participation). In this way logistical objects in the supply chain network can make cash management decisions and place orders autonomously. [70, pp. 20]

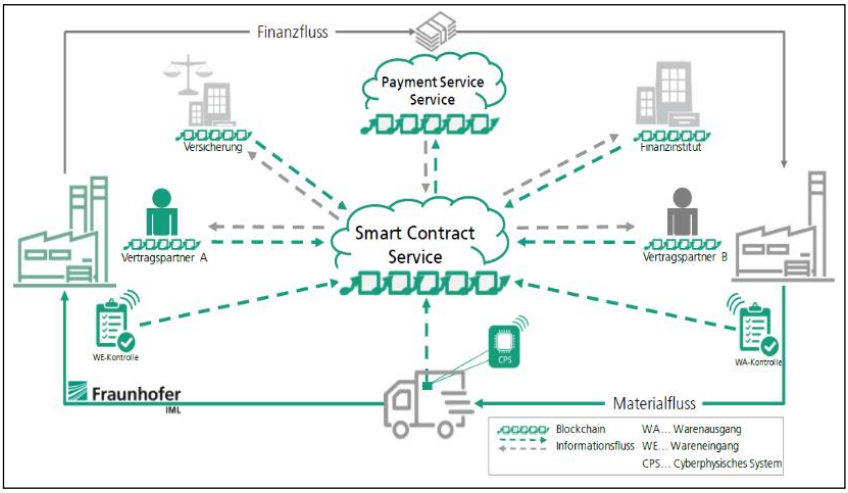


Figure 4: Blockchain in the supply chain management [70, p. 20]

Versicherung = insurance company; Finanzinstitut = bank; Vertragspartner = client; Materialfluss = material flow; WA= outgoing material; WE = incoming material; Kontrolle = control (of)

3.5 Administration

The use of the blockchain technology offers the potential to boost the transparency and credibility of administrative processes and opens up the opportunity to simplify procedures in overall processes, especially at administrative levels, and of internal communication in administrations: in most applications, the government and administration work as intermediaries in order to ensure process flows and transactions. [54] Different registers are kept managing, e.g., ownership structures (property, houses, etc.) or registering births. Depending on the respective context, the technology of the blockchain can allow for more efficient process performance, change already predominant procedures, and resolve partial problems. [86, p. 18]

The potential applications in the public sector are currently under discussion. As figure 5 shows, the debate ranges from e-payments to transparency and openness, publicly kept registers, and the management of ownership structures, all the way to making electronic elections safe. . [70, pp. 24]

Some countries already use blockchains in the public sector: Estonia is internationally considered an exemplary pioneer in this area. It digitizes the entire public administration [64], a process in which the blockchain technology is to play an ever more important role. [56] The city of Zug in Switzerland, which uses blockchain-based e-payments, may serve as another example. Here bitcoins are accepted as payment for administrative fees up to a limit of CHF 200. [60]

For some time the integrity of medical documents has also been secured with a technology that is similar to the blockchain: "Medixain," e.g., is a database where physicians, health insurance companies, and pharmacies can store and access patient data. [49]
In the future, elections can also be conducted via the blockchain system: every citizen receives a token for each vote to be cast, which is then linked to his or her vote. Since the blockchain cannot be manipulated, election fraud can be significantly reduced in this way.

3.6 Crowdfunding

The ICOs presented in chapter 2 are a first issue of asset values by companies where investors as well as customers can acquire these tokens: this makes it a form of crowdfunding. The investors typically receive no property rights in the company, so that by issuing its own cryptocurrency it can build equity in order to fund its own projects, products, or business ideas. Already, platforms exist that offer the opportunity to conduct crowdfunding for startup companies using blockchain technology. Any company can register on the blockchain platform, and the required documents are provided for the companies. This is followed by a brief auditing process. If the company is accepted, the startup can perform the crowdfunding or issue of tokens via the platform. No IT expertise is required, as everything is handled via the platform and decentralization is ensured by the blockchain. [47, 52, 66]
A central point of criticism of ICO funding so far is the high percentage of failed or even deliberately fraudulent projects which, e.g., never intended to follow a serious business model but ultimately only aimed at profiting from the sale of ICOs to the community of ICO enthusiasts hoping for price hikes.

3.7 Further Applications of the Blockchain Technology

Blockchain technology is already employed in various FinTech (financial technology) companies. At the end of 2016, the financial service provider Bitbond, e.g., received a BaFin license. It handles credit transactions among private individuals, so-called P2P lending.
To give another example, R3 CEV heads a consortium consisting of 75 of the world's leading financial institutions and works on a blockchain-based system for processing financial transactions among financial institutes. These use the blockchain solution "Corda." In this context the cryptocurrency Ripple supplies a communication protocol for the banks. This protocol is based on blockchain technology and resembles today's SWIFT protocol.

IBM already presented a blockchain-based trade register, and Everledger is working on a management system for ownership structures of diamonds from their source to their present whereabouts, with the aim of curbing fraud in the diamond trade. [70, pp. 16]
The blockchain can also advance social and societal skills: "Platform operators such as Facebook, Google, Amazon, or Expedia, which so far have had a near monopoly on the Internet, will lose their key position as intermediaries and thus ultimately also their position of predominance. This is a development which sheds new light on the advertising ban for blockchain startups that was recently imposed by Facebook and Google." [49] The browser "Brave," e.g., blocks advertisements when websites are accessed; users who turn off this blocking function receive digital bonus points in return. This signifies a demonopolization of the profit model of advertising: the consumer is rewarded for putting up with the nuisance of advertising—an option that is hardly desirable for the above-mentioned companies like Facebook, Google, Amazon, etc., which therefore may perceive the blockchain also as a threat to their business models. [49]
In addition, it is also possible to use specific reward systems (allotted tokens) via the blockchain to push consumers to assume specific behaviors toward a social, ecological, or other goal: in developing countries, e.g., the "Plastic Bank" [68] exchanges old plastic for tokens which can be used to buy food; the tokens are refinanced through the sale of the recycled plastic.
Other possibilities of the blockchain in the area of environmental protection is "grid singularity," which controls a more efficient use of energy or the volume of emissions, such as CO_2, via a decentralized trading platform: users who access electricity at specific times or take the bike to work would be able to receive "climate coins", which in turn can, e.g., be consolidated and sold to companies as CDO emission certificates. [49]
In development policy, blockchain technology could considerably increase the transparency and effectiveness of project funding, as here, too, payments could be tied to specific targets or other criteria via smart contracts in order to reduce the tremendous risk of project failure (e.g., of World Bank projects on account of corruption and mismanagement [35, pp. 299; 34, chapter 4.3]), which has been very high especially in this area. It is an approach which Germany's KfW, e.g., is pursuing with its idea of a "trusted budget expenditure regime." [67]

4 Risks in Using Cryptocurrencies

4.1 Technical Risks

The cryptographic algorithms which are used in the Bitcoin network are the same as those used on the Internet in many other applications. Diverse transmission channels on the Internet can be found in emails, online payment services, virtual private networks (VPNs), or when a website is accessed. [45, p. 14 f.] Thus the associated technical risks are identical.
The cryptographic algorithm is reflected, for instance, in hash functions and the public key infrastructure (PKI).
The purpose of a hash function is to ensure the integrity of a message. [6, pp. 140] A change and hence a violation of integrity can be detected with a sort of "cross total" across the entire message. The hash function is a one-way function, which means that the original message cannot be retraced from a hash total.

The PKI method serves the encryption and signature of messages. The core elements of the PKI are the public keys (PKs, visible to all network participants) and the private keys (secret keys [SKs], only visible to the owner). Participant A, for instance, can encrypt his message to participant B using her public key (B's PK). Thus only B is able to decode A's message with her private key (B's SK). The sequence in signing messages is reverse. Thus A can sign his message to B with his private key (A's SK), in this way confirming that the message is indeed from A. B can check this using A's public key. [22]

The risk this entails is the theft or loss of the private key. This can happen through phishing attacks (fake emails, text messages, or chats), social engineering (personalized emails containing Trojans, being watched when the password is entered, or by being contacted by phone) or through malware. This happened in January 2018, when hackers looted about US-$ 530 million worth of the cryptocurrency NEM from the crypto exchange Coincheck. [87]

Another risk is pseudonymization, as in the Bitcoin network, for example. A participant is not fundamentally anonymous. He or she only has one or several public addresses in the form of a hash value. Hence participants remain anonymous as long as they do not connect to other online platforms or reveal their identity by having goods sent to their private address or exchanging virtual currency into fiat currency. [8]

Another problem in the blockchain network is scalability. The maximum block size in the Bitcoin network has been set at 1 MB. For Ethereum, blocks no larger than 35 kB have been generated. This means that an average of two transactions per second can be made in the Bitcoin network and seven transactions per second in the Ethereum network.[5] The growing popularity and number of users translates into an increase in transactions per time unit. The two above-mentioned blockchain networks sometimes have trouble processing the large number of transactions. And so, despite the theoretically faster transaction time, this can lead to waiting times of several hours until a transaction is confirmed. [77]

For example, the game CryptoKitties was released in the Ethereum network on 11/28/2017. A mix of Tamagotchi and cryptocurrency, only six days later the blockchain game was responsible for 12% of all transactions in the Ethereum network. This resulted in high transaction fees and long waiting times. [71]

The public blockchains are open source software. Since they are freely accessible, anyone can modify them, implement new functions, and make the changes available to other users. In the blockchain environment the term "fork" is used in this context. A soft fork is a modification of the software which is downward compatible. This means that participants using the old software also accept blocks from participants using the new software. This is different with hard forks: blocks from users with the new software are not accepted and rejected by participants using the old software. This might happen, for instance, when the size of the block increases which users of the old software recognize as invalid. As a consequence, a hard fork results in a split and the formation of two blockchain versions. There have already been over 30 hard forks in the bitcoin network which led to the development of new cryptocurrencies. Only four of them have achieved a market cap worth mentioning as yet (Bitcoin Gold, Bitcoin Cash, Bitcoin Diamond, and Bitcoin Private). [44]

[5] See appendix I

4.2 Economic Risks

4.2.1 Financial Market Stability

According to the Bank for International Settlements, cryptocurrencies contain a threat to financial stability. [31] This is the result of a study by the Kiel Institute for the World Economy. [69, p.15]
Cryptocurrencies are extremely susceptible to speculation risk, as—at least so far—supply and demand are largely not determined by use but for the most part depend on the investors' speculation-related increasing or declining interest. The effects on financial stability resulting from these kinds of speculation waves are the greater the higher the market capitalization rises and the more closely intertwined the crypto markets are with other sectors of the financial and capital markets.
Currencies are protected by central banks and governments, while Bitcoin is not protected. On its website the ECB issues four core statements to warn against the dangers of using bitcoins [34]:

1. Bitcoins are not issued by a central bank which guarantees that you can pay with, say, a ten-euro note in the euro area.
2. Paying with bitcoins is rather complicated. So far there are only few places in your everyday life where you can pay with bitcoins when you go shopping or to a restaurant.
3. In the event of theft or loss of bitcoins, you have no legal protection.
4. Bitcoin is very volatile, which makes it unsuitable for storing value.

4.2.2 Volatility

Figure 5 shows the above-mentioned very high volatility of cryptocurrencies using the example of Bitcoin and gold compared to the US dollar. The great currency fluctuation of Bitcoin to the US dollar, contrary to the relatively stable rate between gold and the US dollar, is immediately evident. One of the reasons might be the great hype around the relatively young technology. Constant media attention attracts investors—all the more so the higher the rate climbs. When profit is taken, the hype turns and there are many (bandwagon) sales. These exaggerated market activities are increased by the very high percentage of inexperienced (small) investors in the area of cryptocurrencies.
Another aspect that helps explain the high volatility is that the crypto markets are subject to occasionally massive attacks in the form of manipulation of the market and currency rates, such as double-spend attacks or spoofing, wash trading strategy, and pumping and dumping (cf. chapter 4.2.3).

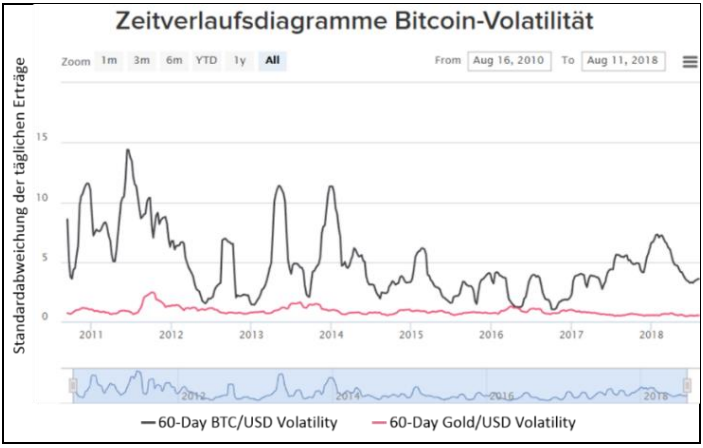


Figure 5: Volatility index US dollar vs. Bitcoin and US dollar vs. gold [20]

4.2.3 Ways of Manipulation

Several studies have detected serious manipulations of prices especially in the wake of the first Bitcoin bubble of 2013. [46] Insider trading is another endemic problem in the Bitcoin system [41], which is also encouraged by the strong concentration of hashing power.

Figure 6 gives an overview of the Bitcoin mining pools:

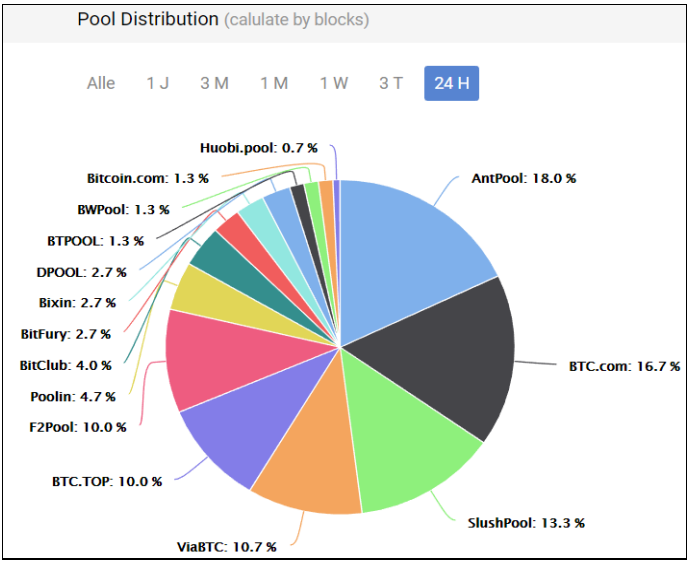


Figure 6: Distribution of the Bitcoin mining pool hash rate [19]

Manipulating transactions through double-spend attacks

Figure 6 shows that the six largest mining pools make up 78.7% of the entire hashing power. This in point of fact constitutes a strong concentration in a theoretically distributed and decentralized network. As a consequence, not only is it easy to make insider arrangements but even to manipulate the blockchain, despite the fact that it is considered insusceptible to manipulation.

Due to the Proof-of-Work consensus algorithm, the hashing power is crucial for determining who generates the next block in the chain and is rewarded for it. The higher the hashing power of the pool, the greater the probability of generating the next block.

This carries the danger of a double-spend attack (also called 51-percent attack). Such an attack aims at spending coins twice. The attacker sells the coins in a transaction on the blockchain. With his superior hashing power he then generates an alternative continuation of the blockchain on which he spends the coins a second time. Thanks to the attacker's hashing power, he can generate more blocks than the rest of the network. Cryptocurrencies such as Bitcoin always accept the chain with the longest series of blocks as valid. All others are rejected as invalid. Such an attack took place on 5/16/2018 and 5/19/2018 in the Bitcoin Gold network, which generated total damage of about US-$18 million. [53]

Another interesting insight is provided by the geographic location of the mining pool. Up to 62% of them are in China [12] (AntPool, BTC.com[6], SlushPool[7], F2Pool, BWPool, Bixin). This, too, indicates a specific kind of concentration in a distributed and decentralized network system, which in view of conceivable future geostrategic confrontations might lead to as yet unforeseen problems.

Manipulating prices

Another major problem of the crypto market is that there are relatively few trading platforms—and "small" ones to boot, in terms of volume—which are more susceptible to price manipulations than, say, the large stock exchanges. Appendix II shows three sample crypto trading platforms. There are some 300 crypto asset funds to date managing a total of some US-$5 billion; yet this market is dominated by only about ten providers—each of which managing approx. US-$100 million—led by Polychain and Pantera. [78] The faster the trading of cryptocurrencies approaches classic trading structures, and the faster conventionally acting funds also enter the crypto market, the smaller will be the possible ways to manipulate it and the volatility of this sector.

A successful strategy for manipulating prices in unregulated crypto markets is so-called spoofing. This refers to a market manipulation strategy where traders flood the market with orders which they then cancel at short notice as soon as the prices have moved in the desired direction. When demand has been generated through spoofing, the trader will sell, but once prices have plummeted as a result of selling orders due to spoofing, they start buying. This method could be observed during as well as after the Bitcoin peaks in late 2017 and early 2028 and is being investigated by the U.S. Department of Justice.

Another price manipulation strategy is the so-called wash trading method: here the fraudulent investor deals with himself in order to suggest demand in the market (which

[6] BTC.com also owns mining pools in Germany

[7] SlushPool also owns mining pools in the USA, Canada, Europe, Singapore and Japan

does not in fact exist) so as to coax other market participants to enter the market—whom he will then be happy to serve.
The pump-and-dump method is also quite popular among the community, whose members make arrangements to this end and coordinate their strategies in social networks: in this way the price of a cryptocurrency is deliberately boosted, e.g., by placing simultaneous purchase orders, which prompts other agents to join in the price rally. Once the previously agreed target price has been reached, the group members sell their coins to still-euphoric third-party buyers, who are then faced with significant losses due to the sudden lack of further orders. [33]

4.2.4 Risk Concerning the Economic Cycle

Economic risks are also considerable—ultimately so considerable that a substitution of government-regulated money by strictly decentralized cryptocurrencies is absolutely impossible.
The great advantage of the cryptocurrencies—that they cannot be randomly increased or reduced—is their final knockout in the context of modern monetary and economic policy: When you choose not to pursue an interest or monetary policy to steer the economy, from a Keynesian standpoint the global economy will once again be pushed into the economic Stone Age of the neoclassical era: economic crises (demand shortfalls) would inevitably lead to a serious recession, perhaps even a depression and strong deflation (= companies regaining their competitiveness through price and wage reductions)—resulting in real mass misery among the population.
A big advantage of cryptocurrencies is considered the fact that—at least in the case of blockchain currencies with a limited volume, such as Bitcoin[8]—they cannot be used to generate a government-manipulated or -generated inflation or even hyperinflation, as in fact often happens, e.g., in Africa and Latin America, but also occurred in Germany in 1923. Unfortunately, this advantage does not go hand in hand with the impossibility of a deflation—rather, the risk of deflation increases exorbitantly compared to regimes with fiat currencies.
The primary risk of deflation lies in the steady increase of the value of the crypto money. As promising as this sounds, it is dangerous, e.g., for debtors: private individuals, debtors, and governments (and hence, once again, private individuals and companies as taxpayers) are in the awkward position of having to put up with debts and wages which remain constant in absolute amounts, which translates into a relative hike in debts and, when the deflation is high enough, inevitably results in overindebtedness.
Deflation slows down the economic development even for debt-free economic units: since prices drop, consumption and investment decisions are deferred, as "everything is becoming cheaper yet." The economy slides into a recession—which exacerbates deflation still more. Without the option of an active fiat monetary policy, such a situation will evolve into an "imbalanced balance" according to Keynes, such as happened worldwide, e.g., in the post-1929 Great Depression.

[8] In the case of in volume-unlimited cryptocurrencies, such as ripple, there is not even this exclusion of inflation, since (theoretically!) large amounts of ripple could be thrown onto the markets in the short term.

A special danger also lies in the fact that cryptocurrencies will automatically—i.e., even without any economic cause—lead to deflation: at the latest when the last bitcoin has been mined[9], a deflation would occur in a Bitcoin money–based economy, even if the economy were still growing: more and more goods transfers would have to be covered from the same money supply: Bitcoin would increase greatly in value, and prices and wages would have to drop accordingly.
The idea of replacing fiat systems by decentralized cryptocurrencies is therefore utterly unrealistic.
What does seem possible, however, is a substitution of the previously "analog" fiat money by national cryptocurrencies: here the cryptocurrency would be controlled centrally by a central bank which could avoid the above-mentioned deflation scenarios (by way of an unlimited cryptocurrency).
It would then also be possible to implement the big advantages of the blockchain technology in the official monetary and payment transactions at a national and international level.
Pending further studies, it would be possible to implement cryptocurrencies in a way that is compatible with a country's national economy. And so a number of central banks are also looking into generating their own cryptocurrency—Estonia might be the first country not only to work on developing a pertinent concept but also to introduce the so-called Estcoin. [56]

4.2.5 Transactions Cost

The transaction costs for conventional payment flows usually differ depending on the type of transfer. They are typically borne by the trader. In credit card payments, they are approx. two to five percent of the transaction amount. In addition, often annual fees are charged. If we take a look at the transaction fees involved with cryptocurrencies, we notice that they are determined by the users themselves. The consensus mechanism of Proof of Work for the definitive legitimization of a blockchain transaction [6, p. 207] is very energy- and cost-intensive. If a user wants to have his or her transaction confirmed as quickly as possible, a higher transaction fee is applied. The motto here is "The one offering the highest amount wins!", i.e., transaction fees depend on the respective number of transactions, and are therefore not necessarily constant or predictable.
What offsets this in terms of an opportunity cost calculation, however, are very short transaction times: a standard transfer via a bank lasts about one day. The duration of a transaction with cryptocurrencies depends on the sequence to which the payment is allocated—if it is assigned to the next block or one after that. Generally speaking, a transaction with cryptocurrencies tends to last approx. 6 to 18 minutes, which makes it considerably faster than conventional transfers and payment flows that take one to two days. [80]

4.2.6 Taxation

Taxation issues appear to be largely unproblematic, as most of them have been cleared up:

[9] The bitcoin, for example, is limited to 20,999,999.9769 BTC. The last Bitcoin block bears the number 6,929,999 and could be generated around the year 2140 [60]

As for sales tax, cryptocurrencies are treated just like legal tender if their only purpose is to be used as a means of payment; according to a verdict of the Court of Justice of the European Union of 10/22/2015, no sales tax is charged for the exchange of national currencies, either. [39, p.1]
Rules have been established for the taxation of revenues: in Germany, e.g., profit realization is tax-free at the end of the twelve-month speculation period; prior to the end of this period the entire profit is subject to the personal income tax rate as long as it is above the exemption limit for private sales (of €600/year). Even if the profit from cryptocurrencies is below this annual exemption limit of €600, it must be listed on the tax return under "Other Income," as the tax exemption has to be confirmed by the Internal Revenue Service in this case, too. [61]

4.2.7 Risk of Loss

Last but not least, the risk of loss is also one of the important economic risks: on the one hand, one may lose one's access data. When you have lost or forgotten your bank card or PIN, you can request a new one from your bank. This is different with cryptocurrencies: if you forget your password or suffer a hardware crash without having made a backup, your assets are permanently lost. Another risk is that the government might decide to declare the currencies illegal, because cryptocurrencies can be used for money laundering and in the Darknet, e.g., or simply because they jeopardize the government's money monopoly.

4.3 Ecological Risks

A major problem with cryptocurrencies is the large amount of energy required for their generation: for Bitcoin alone, in 2017 no less than 215 kWh were spent per transaction for a total of 130 million transactions, approx. 29 TWh (which equals the electricity consumption of Ireland [40]). Currently 90% of the electricity needs are spent on mining new bitcoins, and about 10% for the validation of transactions. [76]
This translates into average transaction costs of the equivalent of €70 in Europe, and in China, of the equivalent of about €23. [40]
The entire energy consumption for mining, not only of bitcoins, increases considerably every year, as the machines computing the algorithm on which the blockchain is based require ever more processing power to mine another (bit)coin: Electricity needs of 70 TWh are expected for Bitcoin for 2018 alone, which already equals the electricity consumption of an industrial nation like Austria.[82, p. 3] Thus cryptocurrencies play no insignificant role in the climate change, as a major portion of the mining transactions takes place in China, where, as we know, regenerative energy still lies somewhere in the future and power generation mostly takes place in coal-fired plants.

4.4 Legal Risks

Blockchain technology entails manifold legal risks which require their own comprehensive analysis. Therefore only a few rudimentary points will be mentioned here: e.g., a transaction which was accepted into the blockchain via a block is irreversibly stored there ("Code Is Law"). Consequently, a legal transaction cannot be annulled and a related contract cannot be rescinded without the contractual partner declaring his or her

consent. The pseudonymous character of the business also makes it difficult to address such a declaration of consent [70, p. 27], so that ultimately there will be no rescission. [8, point 3.7]
Legal transactions may be annulled due to violations of laws or immoral actions. Value judgments of this kind cannot be programmed in smart contracts. Smart contracts merely follow logical links such as “yes” and “no” or “if–then” algorithms.
Another legal means is “provisional ineffectiveness.” It occurs when a contract becomes provisionally ineffective because one business partner is a minor and remains so until a legal representative consents to the effectiveness of the contract (section 108(1) German Civil Code (BGB)). This provisional ineffectiveness cannot be mapped in the blockchain. [83, p. 27]
Another problem is the foreclosure of assets which are stored on the blockchain. Only the user knows the passwords for his or her wallet in the blockchain. Here, too, without the debtor’s active participation there is no way to execute the foreclosure process. What is more, the German Code of Civil Procedure (Zivilprozessordnung, ZPO) only covers the seizure of physical objects (sections 808 et seq. ZPO) and of claims and other property rights (sections 828 et seq. ZPO). Whether and how Bitcoin is covered by these definitions has not been decided yet. [55]
Blockchain technology also entails major obstacles in terms of privacy law. Since data are irreversible once they have been stored in the blockchain, this violates the “right to be forgotten” [70, p. 28] and thus ultimately also the current GDPR [30], which stipulates that individuals have the right to the rectification of their inaccurate (Art. 16 GDPR) and the erasure of their personal data (Art. 17 GDPR). Yet the technology of the blockchain does not permit this.
Even when users only appear with a pseudonym in a blockchain network such as Bitcoin, this does not mean they are entirely anonymous and hence can be found out. If other platforms, such as trading platforms or bank institutions, are linked to the blockchain network through these users, the users can be identified via their shipping address or account number.
Ultimately this means that blockchain technology is only compatible with the General Data Protection Regulation if no personal data are stored or processed on the blockchain any longer. Numerous projects are working on developing solutions to this. [72]

5 Conclusion

Blockchain technology has given rise to a new means of payment: cryptocurrencies. Yet due to the “old” design of its blockchain and very long transaction times, their best known representative, Bitcoin, is already no longer suitable for payment transactions; when it comes to cryptocurrencies, the future therefore belongs to faster, more “modern” altcoins (cf. figures 8 and 9 in Appendix I). Since it is so well known, on the other hand, Bitcoin is currently the best suited among all cryptocurrencies as an investment coin, even though here, too, its extreme volatility compels us to question whether it makes sense to use it for storing value. Moreover, active price manipulations have been documented and are difficult to prevent.
The working hypothesis mentioned at the beginning of this article can thus be confirmed without qualification, especially also on the basis of the economic risks discussed in chapter 3.2:

Thesis 1: "Private cryptocurrencies are inconceivable as an alternative means of payment in the foreseeable future."

A medium of exchange and payment must be able to perform basic functions and possess properties in order to be accepted as a trustworthy currency. [34, chapter 1.2] In particular, it is a crucial requirement that the respective means of payment be accepted by the majority of society. Yet as long as it does not unconditionally serve the purpose of storing value—a basic function of money [69, p. 7]—it is not realistic to assume that it will achieve this wide acceptance.

Therefore the number of cryptocurrency users is still relatively modest. Consequently, in a current survey in Germany by bitkom research, an industry association of 2,600 companies in the digital sector, is shown, that just 4% of people have purchased bitcoins, and 72% are not interested in acquiring any—despite the big hype in 2017. [17] Due to the high volatility of cryptocurrencies, they are currently still not suitable as a means of storing value.

Legally speaking, blockchain technology has yet to overcome obstacles, too. For example, it is impossible to nullify a legal transaction that has been declared invalid, and addressing the responsible parties according to the GDPR is difficult. The right to rectification as well as erasure of personal data is in conflict with the characteristic properties of the blockchain.

What is more, cryptocurrencies are highly susceptible to speculation risks, as supply and demand are largely not determined by use—at least so far—but are guided by the investors' increasing or decreasing interest, which is mostly speculation-driven.

The following plain-spoken quote by the analyst and GMO strategist James Montier is therefore in place here: 'Bitcoin is bullshit. These cryptocurrencies are fascinating but not money. The don't serve any of the classic functions, are not a real medium of exchange, are unsuitable for storing value, and are no unit of account. They are more comparable with stamps or wine—but you can at least drink wine.' [63] This also clarifies that cryptocurrencies have no inherent value whatsoever—unless they are used as ICOs or smart contract tokens.

Which brings us to the second working hypothesis:

Thesis 2: "Increasingly, ICOs can become an alternative to conventional venture capital financing and tokens the driving force to build smart contracts on a decentralized infrastructure."

In addition to their use for cryptocurrencies, blockchains can also be employed to run programs with which smart contracts can be generated—and this will be the primary alternative practical purpose of cryptocurrencies in the future.

Thanks to the open source character of the blockchain, new currencies are constantly being created with all different kinds of functions and properties. For this reason they can also be regarded as technology drivers; as of 8/26/2018 CoinMarketCap listed 1,890 different cryptocurrencies. [25]

On the one hand ICOs are of interest for crowdfunding startups, projects or companies where capital is raised by issuing pertinent tokens. Most importantly, however, in the future smart contracts will require tokens or cryptocurrencies primarily in the Internet of things. Increasingly, this is also the area of application for various research institutions,

such as specifically the Fraunhofer Institutes for Material Flow and Logistics (IML), for Software and Systems Engineering (ISST) as well as the one for Applied Information Technology (FIT); the Horst Götz Institute in Bochum, the European leader in cryptography and IT security research, also merits mention. [67, p. 48]
As they continue to mature and when their initiation is carefully planned, ICOs frequently possess the potential to replace venture capital providers during the initial or early funding phase. However, venture capital providers should not only be regarded in terms of funding: often a valuable transfer of know-how also takes place, access to existing company networks and sales structures is facilitated, or symbiotic partnerships are made between the venture capital provider's company and the startup.
Should the ICO concept become established in this sector in the future as well, this would attract more professional investors and significantly help a company to penetrate the market. In this wake the ties to the conventional banking industry would also be strengthened, which constitutes a catalyst of the risk for the existing financial system that must not be underestimated.
The second working hypothesis mentioned above may therefore be considered verified, especially considering the potential applications for tokens listed in chapter 3: the future of blockchain technology thus might lie less in the creation of a money surrogate but in a digital revolution of diverse applications in everyday life and in or as the Internet of Things.

References

(Last access to the Internet sources on August 26th, 2018)

1. **Aktiendepot.com** (2018): Bitcoins vs. Ripples – zwei Kryptowährungen im direkten Vergleich: https://www.aktiendepot.com/bitcoins-vs-ripples
2. **Avatrade** (2018): Was ist Ripple? https://www.avatrade.de/forex/cryptocurrencies/ripple-trading
3. **Aziz** (2017): Coins, Tokens & Altcoins: What's the Difference? Basics you need to know, in: Master the Crypto: https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/
4. **BaFin** (2017): Blockchain-Technologie: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html
5. **Bergmann, Christoph** (2017): IOTA: Der missverstandene Coin? In: Bicoinblog.de: https://bitcoinblog.de/2017/12/20/iota-der-missverstandene-coin
6. **Berentsen, Aleksander/ Schär, Fabian** (2017): Bitcoin, Blockchain und Kryptoassets. Eine umfassende Einführung, Basel 2017
7. **Bitcoin Cash Symbol** (2018): https://forum.bitcoin.com/bitcoin-cash-f119/bitcoin-cash-logo-branding-t48603.html
8. **Bitcoin.de** (2018): Produktbeschreibung Bitcoins mit Risikoaufklärung: https://www.bitcoin.de/de/produktinformation
9. **Bitcoin.de** Screenshot (2018): Marktübersicht BTC of 26.6.2018, 10:15h: https://bitcoin.de/de

10. **Bitcoin Gold** (2018): Bitcoin Gold (BTG): https://bitcoingold.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf
11. **Bitcoin Gold Symbol** (2018): https://bitcoinblog.de/2017/11/22/bitcoin-gold-so-bekommen-sie-die-neuen-coins
12. **Bitcongress.org** (2018): Best Bitcoin Mining Pools: https://www.bitcongress.org/bitcoin/mining/best-bitcoin-mining-pools/#Top_11_Best_Bitcoin_Mining_Pools_2018
13. **Bitfinex** Screenshot (2018a): Screenshot Teilausschnitt des Tradingtickers auf www.bitfinex.com of 21.5.2018, 17:51h: www.bitfinex.com
14. **Bitfinex** Screenshot (2018b): Handelsübersicht EOS-BTC of 21.5.2018, 17:53h: www.bitfinex.com
15. **Bitkom Research** (2018): Marktforschung für die Digitalwirtschaft. Inzwischen kennen zwei Drittel der Bundesbürger Bitcoin: https://www.bitkom-research.de/epages/63742557.sf/de_DE/?ObjectPath=/Shops/63742557/Categories/Presse/Pressearchiv_2018/Inzwischen_kennen_zwei_Drittel_der_Bundesbuerger_Bitcoin
16. **Blockchaincenter.net** (2018): Verschiedene Typen von Kryptowährungen: https://www.blockchaincenter.net/klassifizierung-von-kryptowaehrungen
17. **BlockchainHub** (2018): Cryptographic Tokens: https://blockchainhub.net/tokens/
18. **Blockchainwelt** (2018): Smart Contracts – Übersicht und Erklärung: https://blockchainwelt.de/smart-contracts-vertrag-blockchain/
19. **BTC.com** (2018): Pool Distribution: https://btc.com/stats/pool?pool_mode=day
20. **Buy Bitcoin Worldwide** (2018): Der Bitcoin Volatilitätsindex: https://www.buybitcoinworldwide.com/de/volatilitatsindex/
21. **ccinvestor** (2018): Die 10 wichtigsten Kryptowährungen: https://ccinvestor.de/die10-wichtigsten-kryptowaehrungen
22. **CGI** (2004): Whitepaper Public Key Encryption and Digital Signature: How do they work?: https://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf
23. **Coinbase** Screenshot (2018): Übersicht Bitcoin: www.coinbase.com of 23.5.2018
24. **CoinMarketCap** (2018a): Global Charts: https://coinmarketcap.com/charts/
25. **CoinMarketCap** (2018b): Alle Kryptowährungen: https://coinmarketcap.com/de/all/views/all/
26. **₡rypto₡oin₩orm** (2018): OmiseGo: https://www.cryptocoinworm.com/currencies/currency/omisego/OMG
27. **Cryptolist** (2018a): Was ist Ethereum? https://www.cryptolist.de/ethereum
28. **Cryptolist** (2018b): Was ist IOTA? https://www.cryptolist.de/iota
29. **Cryptolist** (2018c): Was ist Litecoin? https://www.cryptolist.de/litecoin
30. **Cryptolist** (2018d): What is OmiseGo? https://www.cryptolist.de/omisego
31. **Deutsche Bundesbank** (2018): Carstens: Kryptowährungen können Finanzstabilität gefährden:

https://www.bundesbank.de/Redaktion/DE/Themen/2018/2018_01_31_safe_carstens.html

32. **DGSVO** (2018): Datenschutz-Grundverordnung: https://dsgvo-gesetz.de/
33. **Dörner, Astrid/ Holtermann, Felix** (2018): US-Justiz untersucht Bitcoin-Manipulationen, in: Handelsblatt, No. 99 of 25./26./27.5.2018, p. 32
34. **European Central Bank** (2018): Explainers: What is Bitcoin? https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.en.html
35. **Eibner, Wolfgang** (1991): Grenzen internationaler Verschuldung der Dritten Welt. Restriktionen über Protektionismus, Welthandelsregionalisierung, abnehmende Nettofinanzströme und immanente Wachstumsschwäche: Die ökonomische Begründung des "Debt-relief", Munich 1991
36. **Eibner, Wolfgang** (1996/2003): Grundlagen der Wirtschafts- und Geldordnung, Fernstudienverbund FVL, 1st edition, Berlin 1996, 2nd edition, Berlin 2003
37. **Eibner, Wolfgang** (2008): International Economic Integration: Selected International Organizations and the European Union, Munich 2008
38. **Ethereum Classic Community** (2016): Ethereum Classic Documentation – Release 0.1: https://whitepaperpagoda.files.wordpress.com/2018/02/ethereum-classic.pdf
39. **EuGH-Urteil** vom 22.Oktober 2015 (2015): Umsatzsteuerliche Behandlung von Bitcoin und anderen sog. virtuellen Währungen; EuGH-Urteil vom 22. Oktober 2015, C-264/14, Hedqvist, BStBl 2018 II, pp. 1, Steuern
40. **FAZ, O. V.** (2018): Eine Bitcoin-Transaktion kostet 30 Euro Strom: http://www.faz.net/aktuell/finanzen/digital-bezahlen/bitcoin-eine-transaktion-kostet-30-euro-strom-15282063.html
41. **Feng, Wenjun/ Wang, Yiming/ Zhang, Zhengjun** (2017): Informed trading in the Bitcoin market. In: Finance Research Letters (2017): https://doi.org/10.1016/j.frl.2017.11.009
42. **Finanzen 100** (2018): https://www.finanzen100.de/finanznachrichten/wirtschaft/statistik-so-teilt-sich-der-weltweite-finanzmarkt-auf_H778376918_77478/
43. **Förste, Sebastian** (2018): Wie funktioniert die Startup-Finanzierung durch ICOs? In: Winheller Blog of 4.5.2018: https://winheller.com/blog/startup-finanzierung-icos/
44. **Forks** (2018): Bitcoin Forks. Here you will find an extensive Bitcoin Hard Fork List, Ethereum Hard Fork List, and other Cryptocurrency Hard Fork Lists: https://www.forks.net/list/Bitcoin///2017-01-01/2020-01-01/
45. **Friedman, Milton** (1999): Milton Friedman Full Interview on Anti-Trust and Tech: Interview durch John Berthoud, Vorsitzender der National Taxpayers Union von 1999, veröffentlicht am 09.08.2012: https://www.youtube.com/watch?v=mlwxdyLnMXM

46. **Gandal, Neil/ Hamrick, J. T./ Moore, Tyler/ Oberman, Tali** (2018): Price manipulation in the Bitcoin ecosystem, in: Journal of Monetary Economics (2018): https:// doi.org/10.1016/j.jmoneco.2017.12.004
47. **Handelsblatt** (2018): http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/equity-token-offerings-das-geschaeftsmodell-birgt-auch-risiken/20796494-2.html?ticket=ST-662755-VOkqMollnAutxxAWCdkW-ap1
48. **Higgins, Stan** (2017): 230 Million: Ethereum Classic Community Backs Limit on Total Tokens, in: Coindesk of 1.3.2017: https://www.coindesk.com/230-million-ethereum-classic-community
49. **Hölzner, Heike** (2018): An die Kette legen, in: Handelsblatt, Nr.69 of 12.4.2018, p. 48
50. **Hönig, Michaela** (2018): Initial Coin Offering. Studie zu Kryptowährungen und der Blockchain-Technologie, Studie an der Frankfurt University of Applied Sciences: https://www.frankfurt-university.de/fileadmin/standard/Hochschule/Fachbereich_3/Kontakt/Professor_inn_en/Hoenig/20180502_Bitcoin_Studie_fra_uas_Hoenig_V1.0.pdf
51. **IOTA Symbol** (2018): https://dwglogo.com/iota-logo
52. **Jasch, André** (2017): Crowdfunding trifft auf die Blockchain, in: Companisto: https://www.companisto.com/de/academy/fortgeschrittene/ico-funding-wenn-crowdfunding-auf-die-blockchain-trifft
53. **Kannenberg, Axel** (2018): Bösartiger Miner: 51-Prozent-Attacke und Double-Spend gegen Bitcoin Gold, in: heise online of 25.6.2018: https://www.heise.de/newsticker/meldung/Boesartiger-Miner-51-Prozent-Attacke-und-Double-Spend-gegen-Bitcoin-Gold-4058874.html?wt_mc=rss.ho.beitrag.atom
54. **Killmayer, Jason/ White, Mark/ Chew, Bruce** (2017): Will blockchain transform the public sector? Blockchain basics for government, in: Deloitte University Press. A report from the Deloitte Center for Government Insight: https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf
55. **Kirschbaum, Benjamin** (2015): Insolvenz von Bitcoin-Unternehmen und Staatliche Vollstreckung in Bitcoin-Vermögen, in: Winheller Blog of 29.7.2015: https://winheller.com/blog/insolvenz-bitcoin-unternehmen-vollstreckung-bitcoin-vermoegen/
56. **Klečková, Adéla** (2018): Estcoin: Der neue Star unter den Kryptowährungen? Estland plant die Einführung einer eigenen digitalen Währung, in: Freiheit.org, Analyse, of 31.01.2018: https://www.freiheit.org/estcoin-der-neue-star-unter-den-kryptowaehrungen.
57. **Kryptologen** (2017): Was ist IOTA: https://www.kryptologen.de/2017/07/16/was-ist-iota/
58. **Krypto Magazin** (2018a): Wie lange wird es dauern bis alle Bitcoin generiert sind? https://www.krypto-magazin.de/wie-lange-wird-es-dauern-bis-alle-bitcoin-generiert-sind/

59. **Krypto Magazin** (2018b): Was ist OmiseGo? https://www.krypto-magazin.de/was-ist-omisego-omg
60. **Luzerner Zeitung** (2016): ZUG: 12 Zuger zahlen in der Stadtverwaltung mit Bitcoins, in: Luzerner Zeitung of 15.12.2016: https://www.luzernerzeitung.ch/zentralschweiz/zug/zug-12-zuger-zahlen-in-der-stadtverwaltung-mit-bitcoins-ld.32551
61. **Mazars** (2018): Besteuerung von Bitcoin.Geschäften bei Privatanlegern: https://www.mazars.de/Home/Themen/Nachrichten/Besteuerung-bei-Privatanlegern
62. **Metafinanz** (2017): Expertenkommentare – Corda: Irgendwie Blockchain und irgendwie auch nicht, in Metafinanz – Expertenkommentare vom: 23.11.17: https://metafinanz.de/2017/11/23/corda-blockchain/
63. **Montier, James** (2018): „US-Aktien sind extrem teuer". Einer der ungewöhnlichsten Analysten spricht über ausgereizte Märkte, getriebene Anleger und den Bitcoin als faszinierenden Bullshit, in: Handelsblatt, No. 131 of 11.7.2018, pp. 34 - 35
64. **Müller-Marc, Oliver** (2018): Zukunft Digitalisierung: Was Deutschland von Estland lernen kann, in: Digital Business of 28.4.14: https://ensego.de/blog/zukunft-digitalisierung-deutschland-estland-lernen/
65. **Nakamoto, Satochi** (2008): Bitcoin: A Peer-to-Peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf
66. **Neufund** (2017): Whitepaper v2.0: https://neufund.org/cms_resources/whitepaper.pdf
67. **Pinkwart, Andreas** (2018): Geschützter Austausch, in: Handelsblatt, No. 134 v. 16.7.2018, p. 48
68. **Plastic Bank** (2018): Plastic Bank stopps Ocean Plastic while reducing Poverty: https://www.plasticbank.org/what-we-do/
69. **Policy Department for Economic, Scientific and Quality of Life Policies (Hrsg.)** (2018): In-Depth Analysis, Requested by the ECON Committee: Fiedler/ Gern/ Herle/ Kooths/ Stolzenburg/ Stoppok: Virtual Currencies – Monetary Dialogue July 2018, Studie des Kieler Weltwirtschaftsinstitutes – Kiel Institute for the World Economy, Kiel, Brüssel 2018
70. **Prinz, W./ Schulte, A**. (Hrsg.) (2017): BLOCKCHAIN. Technologien, Forschungsfragen und Anwendungen; Positionspapier der Fraunhofer Gesellschaft: https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/FhG-Positionspapier-Blockchain.pdf
71. **Quartz** (2017): The Ethereum network is getting jammed up because people are rushing to buy cartoon cats on its Blockchain: https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion/
72. **Rödder, Valerie** (2018): Datenschutzgrundverordnung: So wirkt sich die DSGVO auf die Blockchain aus, in: base 58.de Decoding Blockchain, of 24.5.2018: https://base58.de/datenschutz-grundverordnung-dsgvo-und-die-blockchain/

73. **Schär, Fabian** (2017): Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung (2016), Books on Demand
74. **Schlatt, Vincent/ Schweizer, André/ Urbach, Nils/ Fridgen, Gilbert** (2016): Whitepaper Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth, 2016
75. **Schmeh, Klaus** (2016): Kryptografie: Verfahren, Protokolle, Infrastrukturen, 6th edition
76. **Schock, Stephanie** (2018): Katastrophale Umweltbilanz von Bitcoin: https://blog.de.erste-am.com/2018/02/12/katastrophale-umweltbilanz-von-bitcoin/
77. **Simonite, Tom** (2017): Der Bitcoin macht nicht mehr, was er einmal sollte: https://www.wired.de/collection/business/bitcoin-macht-nicht-mehr-das-was-er-einmal-sollte
78. **Slodczyk, Katharina** (2018): Blockchain. Der lange Weg zur Marktreife, in: Handelsblatt, No. 107 of 7.6.2018, p. 31
79. **Spancken, Marius/ Mario Hellenkamp, Mario/ Brown, Christopher/ Thiel, Christian** (2016): Abschlussbericht zum Forschungs- und Entwicklungsprojekt 2015/2016 im Studiengang Master of Science Wirtschaftsinformatik an der FH Münster: Kryptowährungen und Smart Contract: https://www.hb.fh-muenster.de/opus/fhms/volltexte/2016/1246/pdf/FuE_Kryptowaehrungen_und_Smart_Contracts_Abschlussbericht.pdf
80. **Sparkassenfinanzportal** (2018): Wie lange dauern Überweisungen in Deutschland? https://www.sparkasse.de/geld-leichter-verstehen/w/wie-lange-dauern-uberweisungen-deutschland.html
81. **Statista** (2018) Wertentwicklung der weltweit an den Börsen gehandelten Aktien von 1980 bis 2017: https://de.statista.com/statistik/daten/studie/199488/umfrage/wert-des-weltweiten-aktienbestandes-seit-2000/
82. **Stocker, Frank** (2018): Bitcoin-Crash hat 600 Mrd. Dollar ausradiert: https://welt.de/181217212
83. **Süme, Oliver/ Vogt, Jan Niklas/ Zimprich, Stephan** (2018): Rechtliche Rahmenbedingungen der Blockchain, in: VDI Technologiezentrum (Hrsg.), März 2018: Blockchain – Eine Technologie mit disruptivem Charakter: https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Meldungen/2018/Blockchain_-_Eine_Technologie_mit_disruptivem_Charakter.pdf, p. 27 – 28
84. **The Motley Fool** (2017): Vergleich der Marktkapitalisierungen von Bitcoin mit Gold, dem S&P 500 und dem amerikanischen Dollar: https://www.fool.de/2017/08/22/vergleich-der-marktkapitalisierungen-von-bitcoin-mit-gold-dem-sp-500-und-dem-amerikanischen-dollar/
85. **Voshmgir, Shermin** (2016): Blockchains, Smart Contracts und das Dezentrale Web, in: Technologiestiftung Berlin (Hrsg.): https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf

86. **Welzel, Christian/ Eckert, Klaus-Peter/ Kirstein, Fabian/ Jacumeit, Volker** (2017): Mythos Blockchain: Herausforderung für den öffentlichen Sektor, in: Kompetenzzentrum Öffentliche IT: https://cdn0.scrvt.com/fokus/1ce7946ad1882e46/18ab9d5982ef/Mythos-Blockchain---Herausforderung-f-r-den--ffentlichen-Sektor.pdf

87. **Wirtschaftswoche** (2018): https://www.wiwo.de/finanzen/geldanlage/hackerangriff-auf-coincheck-so-reagieren-die-behoerden-auf-den-mega-raub/20902810.html

88. **Zetzsche, Dirk A./ Buckley, Ross P./ Arner, Douglas W./ Föhr, Linus**, (2018): The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298

Appendix I: Relevant Cryptocurrencies

	BITCOIN	BITCOIN GOLD	BITCOIN CASH	LITECOIN	DASH
Begrenzung:	21 Mio.	21 Mio.	21 Mio.	84 Mio.	5,3 Mio.
Transaktionszeit	10 min.	10 min.	10 min.	2,5 sec.	1,3 sec.
Bockgröße:	1 MB	1 MB	12 MB	1 MB (+)	2 MB
Verwendungs-zweck	Zahlungssystem	Zahlungs- und Anlage-möglichkeit	Zahlungsystem mit höheren Blockgrößen-limits gegenüber Bitcoin	Verwaltung von Transaktionen, Bilanzen und Ausgaben	private, schnelle und anonyme Transaktionen
Technologie:	Blockchain	Blockchain	Blockchain	Blockchain	Blockchain

Figure 7: Relevant cryptocurrencies, part 1
(Own compilation of [7, 8, 10, 11, 21, 26, 27, 29, 59])

	Ethereum	Ethereum Classic	Ripple	IOTA	Omise GO
Begrenzung:	Keine (evtl.120 Mio.??)	230 Mio.	100 Mrd.	2,8 Mrd.	Keine
Transaktions-zeit:	12 sec.	15 sec.	3-5 sec.	10 sec.	< 1 sec.
Verwendungs-zweck:	Finanzgeschäfte, Kapitalmarkt	Investment, Zahlungsmittel für Rechenleistung	Open-Source-Protokoll für Zahlungsnetz-werke	Kommunikations- und Zahlungs-Medium für Internet of Things (IoT)	E-Wallets, Zahlungsmittel, automatische Konvertierung in Zielwährung
Technologie:	Blockchain & Smart Contracts	Blockchain & Smart Contracts	Blockchain	Tangle	Ethereum - Blockchain

Figure 8: Relevant cryptocurrencies, part 2
Own compilation of [1, 5, 21, 28, 30, 38, 48, 51]

Appendix II: Sample Trading Platforms

Bitcoin.de: **The most important platform in the German-speaking countries and the most significant European trading platform for Bitcoin and Ethereum**

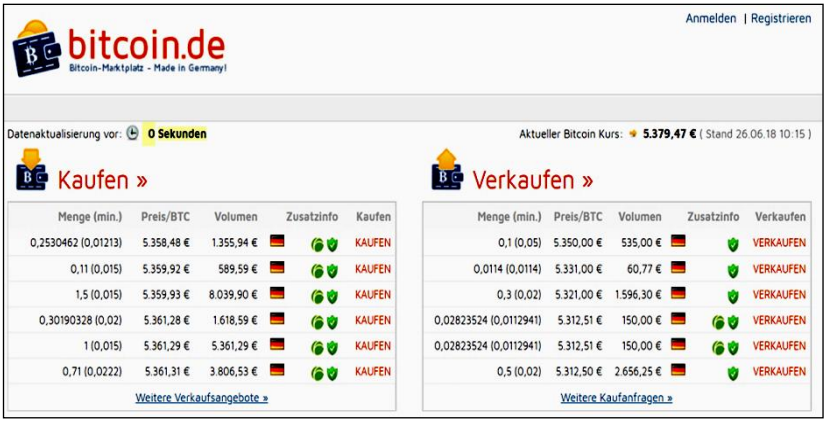


Figure 9: Screenshot of www.bitcoin.de [9]

Country: Germany **Market volume:** > €5 million/day
Currencies traded: 4: Bitcoin, Bitcoin Gold, Bitcoin Cash, Ethereum

Coinbase.com: the most relevant U.S. trading platform for cryptocurrencies

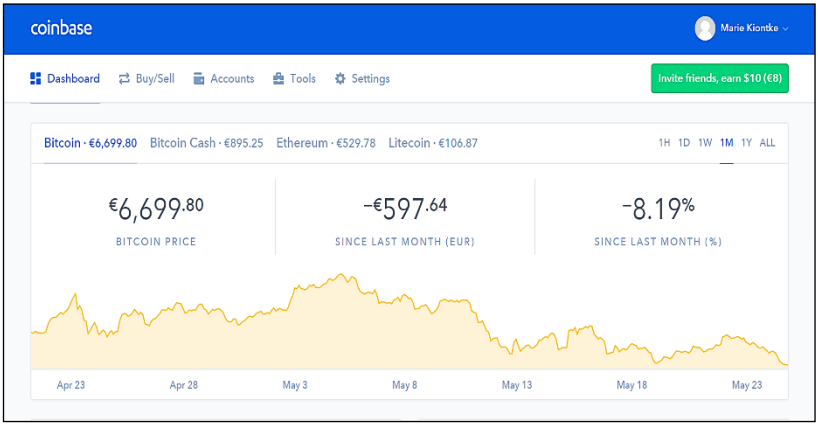
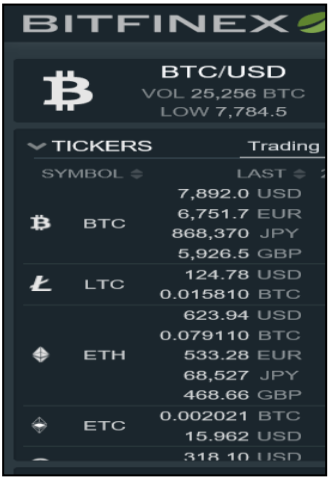


Figure 10: Screenshot of www.coinbase.com [23]

Country: USA **Market volume:** >US-$ 800 million/day
Currencies traded: >10

Bitfinex.com: **The second-largest trading platform for cryptocurrencies and currencies**



Country: China, Hong Kong

Market volume: US-$2.4 billion/day

Currencies traded: >80, constantly expanding

Figure 11: Screenshot of part of the trading ticker on www.bitfinex.com [13]

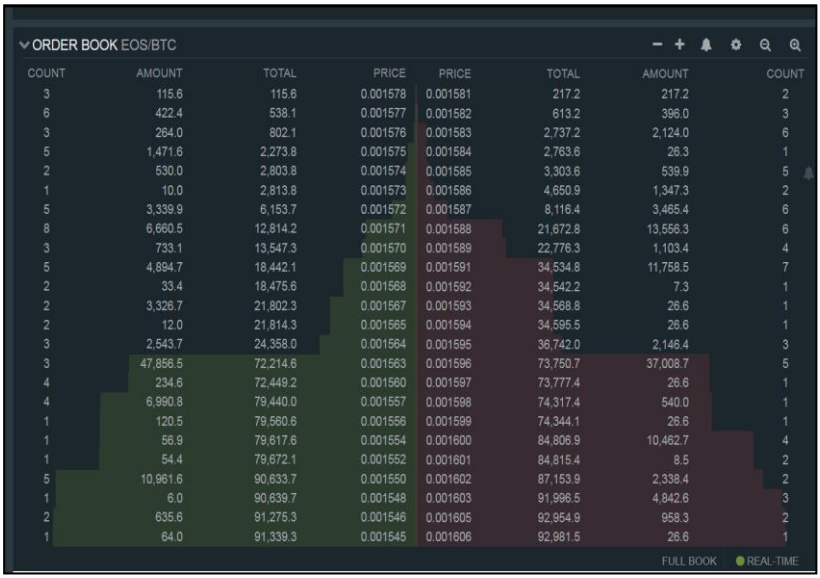


Figure 12: Screenshot of supply and demand using the example of a trade with EOS and Bitcoin on www.bitfinex.com [14]